AO 106 (Rev. 04/10) Application for a Search Warrant

AUSA Jessica Kim

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Property secured from the person of
ANDREW K. MITCHELL
DOB: 12/01/1963, SSN: 293-46-1619

Case No. 2:18mj739

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B and/or attached Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 242	Deprivation of rights under color of law
18 U.S.C. 1951	Hobbs Act extortion

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Robert D. Bogner, Task Force Officer, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9-27-18

Judge's signature

City and state: Columbus, Ohio

Hon. Chelsey M. Vascura, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF: **Property secured from the person of** **ANDREW K. MITCHELL** **DOB: 12/01/1963** **SSN: 293-46-1619** **on September 26, 2018 at John Glenn Columbus International Airport**	**Case No.** 2:18mj739

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Robert D. Bogner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the property secured from the person of Andrew K. MITCHELL, DOB: 12/01/1963, SSN: 293-46-1619 on September 26, 2018 at John Glenn Columbus International Airport, hereinafter "PROPERTY," further described in Attachment A, for the things described in Attachment B.

2. I am an Inspector with the Ohio Auditor of State (AOS), where I have worked since February 2015. As an AOS Inspector, I am responsible for conducting criminal investigations involving theft, theft in office, public corruption, and other violations of law. Since February 2017, I have been deputized as a Task Force Officer with the Federal Bureau of Investigation (FBI), Columbus Resident Agency for the Southern District of Ohio, Eastern Division. I am currently assigned to the Public Corruption Squad. As such, I am an

"investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am an officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated in 18 U.S.C. § 2516.

3. Prior to working as an AOS Inspector, I was a Special Agent with the Internal Revenue Service Criminal Investigation (IRS-CI) for 28 years. During that time, I investigated violations of the Internal Revenue laws and related offenses and was involved in numerous investigations involving violations of the United States Code. I have provided financial investigative expertise and assistance to various federal and local agencies, including the FBI, Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, and Firearms (ATF), and the Columbus Division of Police Narcotics Bureau.

4. During my tenure as a Task Force Officer with the FBI, I have been assigned to work on various types of investigations, including public corruption, financial crimes, violent crimes, narcotics offenses, and money laundering. I have experience in the execution of search warrants and the debriefing of defendants, witnesses, informants, and other persons who have knowledge of various types of illegal activities. I have experience in the use of sophisticated investigative techniques to include electronic surveillance, GPS tracking devices, telephone tracking, and wiretaps.

5. I, along with other agents and officers from the FBI, the Columbus Division of Police (CPD), the Ohio Bureau of Criminal Investigation (BCI), and the Ohio Auditor of State (AOS), have been investigating corruption in the Columbus Division of Police Department's Vice Unit involving CPD Vice Unit Detective Andrew K. Mitchell. Over the course of this investigation, I have become familiar with the organization and structure of the CPD Vice Unit, as well as the nature and scope of the CPD Vice Unit's duties.

6. The facts set forth below are based upon my own observations and experience with this investigation, as well as investigative reports and information provided to me by other federal and state law enforcement officers. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

7. Based on my training and experience, as well as information obtained from (i) interviews with sources of information and other witnesses; (ii) investigative reports and arrest records; (iii) federal and state law enforcement officers; (iv) public database searches; and (v) the ongoing investigation of the CPD Vice Unit in this district, there is probable cause to believe that violations of 18 U.S.C. § 242 (deprivation of rights under color of law) and 18 U.S.C. § 1951 (Hobbs Act extortion) have been committed by CPD Vice Unit Detective Andrew K. MITCHELL.

8. On September 26, 2018, a series of search warrants were judicially authorized by this Court, including but not limited to:

a. **2:18-mj-730** – 6249 Howard Road, Sunbury, Ohio 43074;

b. **2:18-mj-731** – 2013 Cadillac XTS, VIN #2G61P5S32D9107621, Ohio License Plate #EPJ9719;

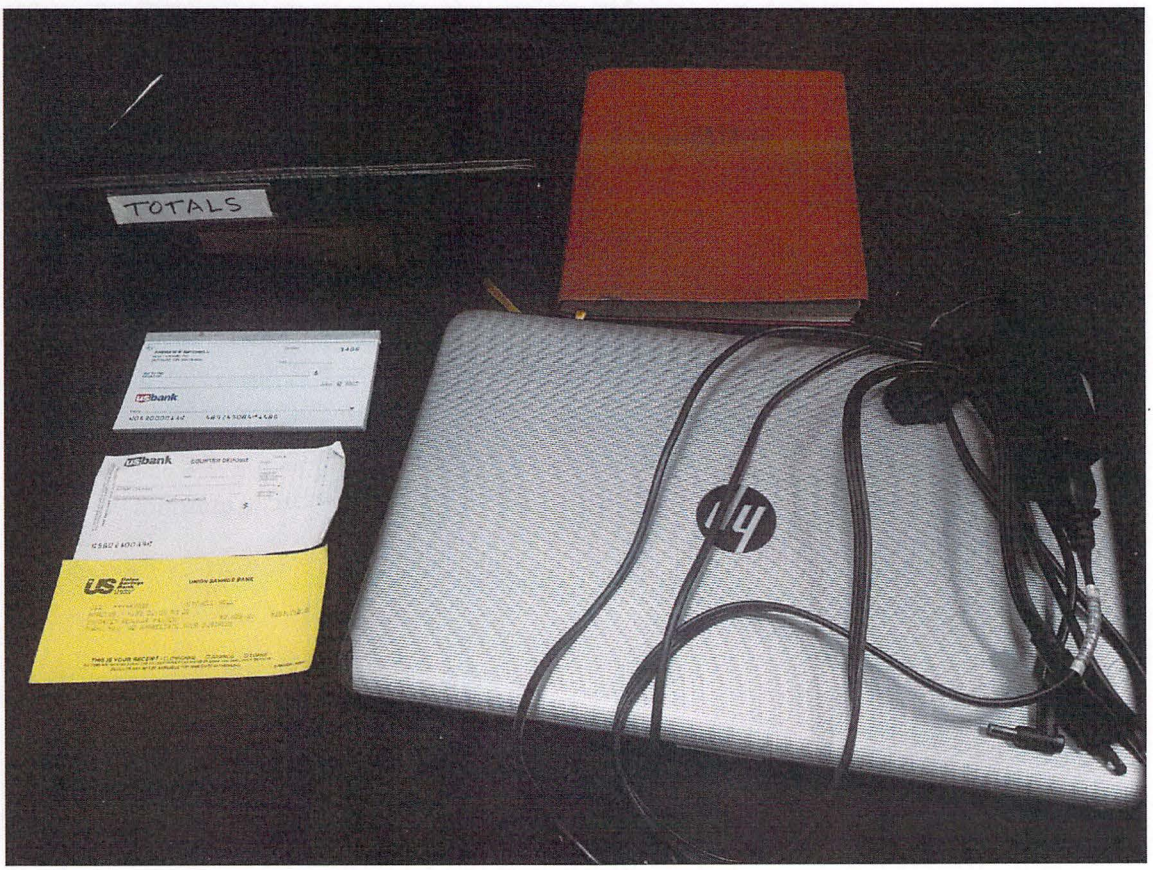
c. **2:18-mj-732** – 2015 Lincoln Navigator, VIN #5LMJJ2JT1FEJ01610, Ohio License Plate #GLX6189;

d. **2:18-mj-733** – The person of Andrew K. MITCHELL for cellular telephone IMEI #355989088596379, ESN #089506023208754743, with assigned cellular telephone number 614-679-0788 serviced by Sprint; and

e. **2:18-mj-734** – The person of Andrew K. MITCHELL for DNA and photographic evidence.

Your Affiant hereby incorporates the affidavits of those judicially authorized search warrants into this affidavit.

9. On September 26, 2018, the judicially authorized search warrants discussed above were executed. During the execution of the judicially authorized search warrants for the person of Andrew K. MITCHELL (2:18-mj-733 and 2:18-mj-734), MITCHELL was encountered at John Glenn Columbus International Airport, located at 4600 International Gateway, Columbus, Ohio 43219, where he was scheduled to fly out on Spirit Airlines flight number 325 departing at 7:45pm to Las Vegas. During this encounter, MITCHELL was unexpectedly found in possession of the following PROPERTY on his person: one (1) HP laptop computer (serial number CND6379GNM), one (1) black notebook/binder, one (1) brown planner, and various bank records (including checks and bank slips), as shown in the photo below:



10. In conjunction with the execution of the judicially authorized search warrants for the person of Andrew K. MITCHELL (2:18-mj-733 and 2:18-mj-734) at John Glenn Columbus International Airport, investigators were also executing the judicially authorized search warrant (2:18-mj-730) at MITCHELL's primary residence, located at 6249 Howard Road, Sunbury, Ohio 43074. There, MITCHELL's wife, Tanya Mclymont Mitchell, told investigators that MITCHELL retains records regarding his rental properties on the HP laptop (part of the PROPERTY) that was found on his person during the encounter discussed above at John Glenn Columbus International Airport. Your Affiant re-highlights the following facts from the previously authorized and incorporated affidavits:

a. A search of the Franklin County Auditor and Recorders Office websites revealed that MITCHELL has purchased and/or sold over 40 rental properties since the 1990s, and currently owns approximately 16 properties.

b. This investigation has identified several prostitutes who engaged in sex acts for money with MITCHELL and/or were tenants in MITCHELL's rental properties.

c. During the course of this investigation, investigators have learned of at least two women who posted on social media that they had rented properties from MITCHELL, and that he had propositioned them for sex in exchange for rent.

11. Pursuant to the authority given under the previous judicially authorized search warrants, investigators secured the PROPERTY and are awaiting authority from the Court to search and seize. If the Court is unwilling to grant search and seizure authority, investigators will promptly return the PROPERTY to MITCHELL and/or his designated family member.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

12. As described above and in Attachment B, this application seeks permission to search for records that might be found in the PROPERTY, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

13. *Probable cause.* I submit that if a computer or storage medium is found in the PROPERTY, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

14. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PROPERTY because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where,

and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and

intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer as an instrumentality to commit a crime, particularly over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may

contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

15. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge

that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

16. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

17. Based on the information provided in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 242 (deprivation of rights under color of law) and 18 U.S.C. § 1951 (Hobbs Act extortion) have been committed and/or are being committed. I submit that this affidavit supports probable cause for a warrant to search the PROPERTY described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Robert D. Bogner
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on September 27, 2018.

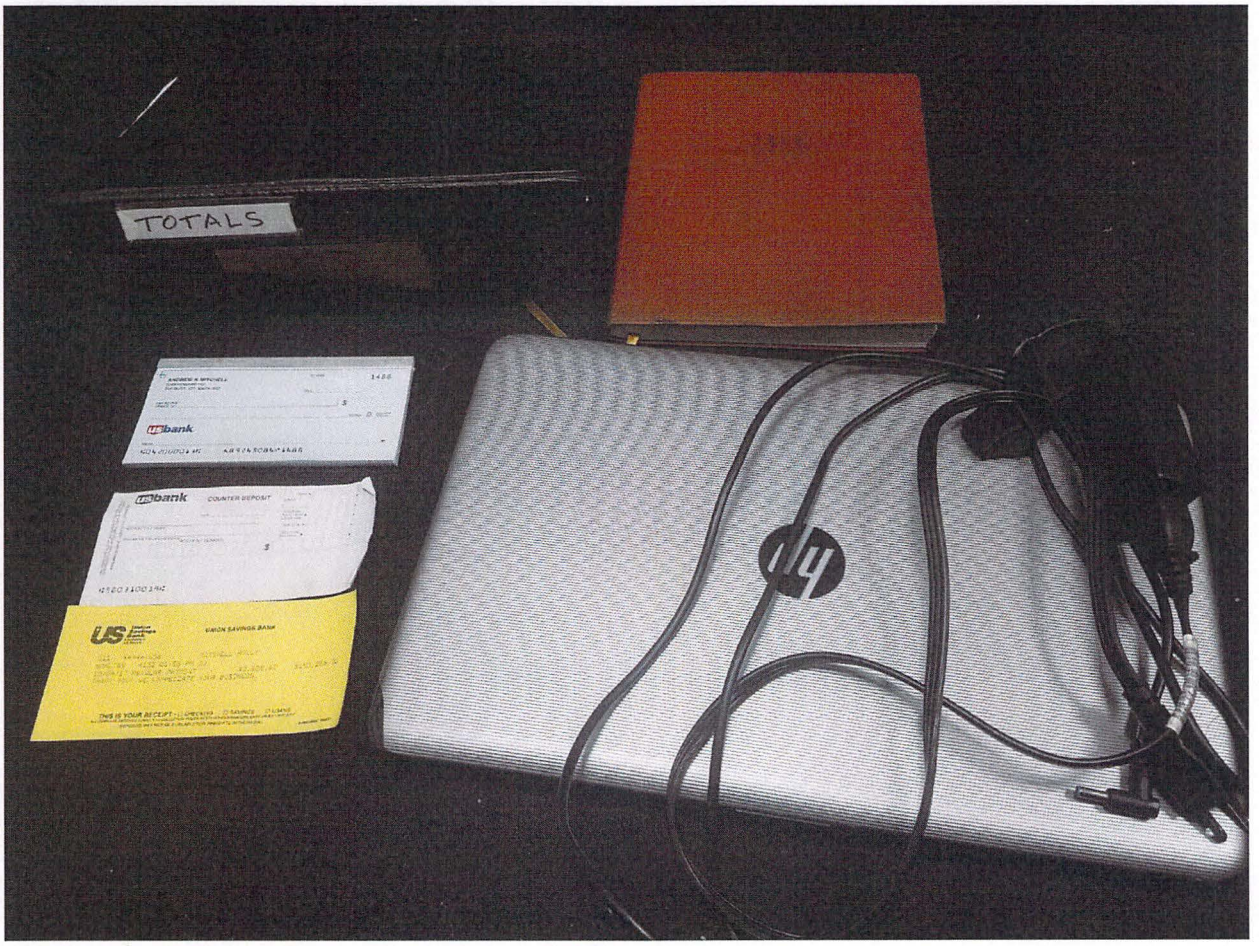
Honorable Chelsey M. Vascura
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The PROPERTY to be searched is the following, as shown in the photo below:

- One (1) HP laptop, silver/black in color, serial number CND6379GNM;
- One (1) black notebook;
- One (1) brown planner; and
- Bank records, including checks and bank slips.



ATTACHMENT B

PROPERTY TO BE SEIZED

1. All records relating to violations of 18 U.S.C. § 242 (deprivation of rights under color of law) and/or 18 U.S.C. § 1951 (Hobbs Act extortion), including but not limited to:

   a. Records and information relating to indicia of ownership, possession, control, or dominion over the location described in Attachment A, as well as vehicles located thereon, including but not limited to deeds, purchase/lease agreements, land contracts, titles, and vehicle registrations;

   b. Records and information relating to financial institutions and other individuals or businesses with whom a financial relationship exists,

   c. Records and information relating to the receipt, deposit, or transmission of funds of any kind, including but not limited to bank records, checks, deposit tickets, money orders, wire transfers, credit card bills, account information, receipts, and other financial records and information;

   d. Records and information relating to cellular phone usage or electronic device usage, including account statements and call detail records, as well as indicia of the use or ownership of same;

   e. Records and information relating to e-mail accounts and social media accounts, as well as indicia of the use or ownership of same;

   f. Records and information relating to real estate transactions, tenant listings, invoices, receipts, records of eviction, and tax returns;

g. Records and information relating to names, addresses, telephone numbers, and other contact information of tenants/victims, including but not limited to logs, notebooks, ledgers, planners, notes, and other documents and records identifying victims/tenants, as well as photographs, videotapes, film, undeveloped film and the contents therein;

h. Records and information relating to the identity or location of any additional suspects;

i. The opening, search, and removal, if necessary, of any safe or locked receptacle or compartment, as some or all of the property heretofore may be maintained;

j. Records and information relating to any storage facilities;

k. Any and all other records or information relating to violations of 18 U.S.C. § 242 (deprivation of rights under color of law), 18 U.S.C. § 1951 (Hobbs Act extortion), and related offenses.

2. Computers, cellular telephones, tablets, personal data devices, electronic devices, or storage media used as a means to commit the violations described above, as well as indicia of the use or ownership of same.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.